

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of
The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.



DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITE DE COOPERATION EN MATIÈRE DE BREVETS (PCT)

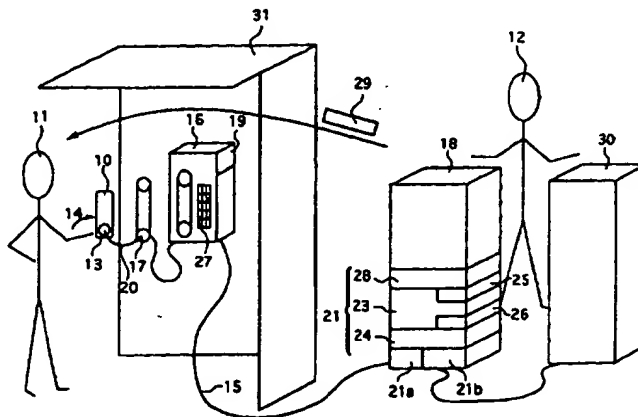
(51) Classification internationale des brevets ⁶ : H04M 3/38, 15/00, 17/00	A2	(11) Numéro de publication internationale: WO 98/13990 (43) Date de publication internationale: 2 avril 1998 (02.04.98)
(21) Numéro de la demande internationale: PCT/FR97/01683 (22) Date de dépôt international: 25 septembre 1997 (25.09.97) (30) Données relatives à la priorité: 96/11914 25 septembre 1996 (25.09.96) FR (71) Déposant (pour tous les Etats désignés sauf US): FINTEL S.A. [FR/FR]; 87, boulevard Haussmann, F-75008 Paris (FR). (72) Inventeurs; et (75) Inventeurs/Déposants (US seulement): ROSSET, Franck [FR/FR]; 96, boulevard Beaumarchais, F-75011 Paris (FR). GAYET, Alain [FR/FR]; 13, place des Dominos, F-92400 Courbevoie (FR). MOULIN, Jean [FR/FR]; 5, avenue de Beauséjour, F-92210 Draveil (FR). (74) Mandataire: VIDON, Patrice; Cabinet Patrice Vidon, Im- meuble Germanium, 80, avenue des Buttes de Coësmes, F-35700 Rennes (FR).		(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, KE, LS, MW, SD, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Publiée <i>Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.</i>

(54) Title: METHOD AND SYSTEM FOR ENSURING THE SECURITY OF THE SUPPLY OF SERVICES OF TELECOMMUNICATION OPERATORS

(54) Titre: PROCEDE ET SYSTEME POUR SECURISER LES PRESTATIONS DE SERVICE DES OPERATEURS DE TELECOMMUNICATION

(57) Abstract

The invention concerns a method and a system enabling a telecommunication operator (12) to identify rapidly and to debit in complete security the accounts of subscribers of a telephone network. The method comprises the following steps: the telecommunication operator (12) provides each of its subscribers (11) with a subscriber card (10), formatted like a credit card, personalised by specific identifiers for each subscriber and for each subscriber card; said card (10), formatted like a credit card, emits brief identifying sound signals, of the DTMF type, at least partly encrypted, varying with each operation, when it is actuated (14) by the customer (11); the sound signals are received by the microphone (17) of the handset (16) and are converted into electric signals, before being transmitted by the communication network (15) to the computer service (18) of the telecommunication operator (12); the transmitted signals are electronically processed and decrypted (24) by the computer service (18) of the telecommunication operator (12) and the data obtained after processing are compared (25) to the identification data of the subscriber and the subscriber card in the possession of the computer service (18) of the telecommunication operator.



(57) Abrégé

L'invention concerne un procédé et un système permettant à un opérateur (12) de télécommunication d'identifier de manière rapide et de débiter de manière sûre les comptes des abonnés d'un réseau téléphonique. Le procédé comprend les étapes suivantes: l'opérateur de télécommunication (12) met à la disposition de chacun des abonnés (11) une carte d'abonné (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte d'abonné; ladite carte (10), au format carte de crédit, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée (14) par l'abonné (11); les signaux acoustiques d'identification sont reçus par le microphone (17) du combiné téléphonique (16) et sont convertis en signaux électriques, avant d'être transmis par le réseau de communication (15) au service informatique (18) de l'opérateur de télécommunication (12); les signaux transmis sont traités et décryptés (24) électroniquement par le service informatique (18) de l'opérateur de télécommunication (12) et les données obtenues après traitement sont comparées (25) aux données d'identification de l'abonné et de la carte d'abonné détenues par le service informatique (18) de l'opérateur de télécommunication.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce	ML	Mali	TR	Turquie
BG	Bulgarie	HU	Hongrie	MN	Mongolie	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MR	Mauritanie	UA	Ukraine
BR	Brésil	IL	Israël	MW	Malawi	UG	Ouganda
BY	Bélarus	IS	Islande	MX	Mexique	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	NE	Niger	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NL	Pays-Bas	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norvège	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NZ	Nouvelle-Zélande	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	PL	Pologne		
CM	Cameroun	KR	République de Corée	PT	Portugal		
CN	Chine	KZ	Kazakhstan	RO	Roumanie		
CU	Cuba	LC	Sainte-Lucie	RU	Fédération de Russie		
CZ	République tchèque	LI	Liechtenstein	SD	Soudan		
DE	Allemagne	LK	Sri Lanka	SE	Suède		
DK	Danemark	LR	Libéria	SG	Singapour		
EE	Estonie						

**PROCEDE ET SYSTEME POUR SECURISER LES PRESTATIONS DE SERVICE DES OPERATEURS DE TELECOM-
MUNICATION**

Le domaine de l'invention est celui des prestations de service à distance proposées par les opérateurs de télécommunication à leurs clients abonnés à leur réseau.

5 Plus précisément l'invention concerne un procédé et un système permettant à un opérateur de télécommunication d'identifier de manière rapide et de débiter de manière sûre les comptes des abonnés d'un réseau téléphonique.

Le problème posé est d'empêcher un utilisateur mal intentionné d'accéder au réseau de télécommunication sans y être autorisé, sans acquitter les droits correspondants ou en
10 prétendant qu'il n'a pas demandé les services qui lui sont débités par l'opérateur de télécommunication.

Pour résoudre ce problème il a été proposé d'utiliser des clés d'accès générées par des cartes à mémoire et de modifier les combinés téléphoniques pour qu'ils puissent lire les cartes à mémoire. Ces solutions, outre leur coût, sont peu pratiques et longues à mettre en
15 oeuvre. En fait, le problème posé ne peut être effectivement résolu que si on sait résoudre simultanément un autre problème : concevoir un procédé et un système commode d'utilisation, rapide à mettre en oeuvre et économique. En effet, dès lors que l'on s'adresse à un large public, la facilité d'utilisation et les gains de temps deviennent des problèmes majeurs qui ne peuvent pas être écartés.

20 Il a été proposé (document WO 96 04741 au nom de Andrew MARK) d'utiliser une carte émettant des signaux acoustiques, cryptés, de type DTMF. Ainsi, le porteur d'une telle carte, en accouplant celle-ci au microphone du combiné téléphonique transfère automatiquement aux services informatiques, ses identifiants. Comme ces identifiants sont chiffrés, on peut penser qu'un tiers ne sera pas en mesure d'en comprendre le
25 contenu. Toutefois, l'enregistrement des signaux émis par la carte reste possible et un fraudeur muni d'un tel enregistrement peut se substituer au bénéficiaire de la carte.

La solution de A. MARK, si elle était transposée dans le cas des opérateurs de télécommunication, afin d'identifier de manière rapide et sûre les abonnés de leurs réseaux, ne permettrait donc pas d'empêcher un utilisateur mal intentionné d'accéder,
30 sans y être autorisé, aux services offerts par les opérateurs de télécommunication.

Les objectifs visés par la présente invention sont atteints et les problèmes que posent les techniques selon l'art antérieur sont résolus, selon l'invention, à l'aide d'un procédé comprenant les étapes suivantes :

5 - l'opérateur de télécommunication met à la disposition de chacun des abonnés une carte d'abonné, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte d'abonné,

- la dite carte, au format carte de crédit, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée par l'abonné,

10 - les signaux acoustiques d'identification sont reçus par le microphone du combiné téléphonique et sont convertis en signaux électriques, avant d'être transmis par le réseau de communication au service informatique de l'opérateur de télécommunication,

15 - les signaux transmis et les données d'identification du client et de la carte détenues par le service informatique sont traités et comparés électroniquement par le service informatique de l'opérateur de télécommunication.

Ainsi, grâce à ce procédé, l'opérateur de télécommunication peut vérifier que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'il offre. De sorte qu'en cas de conformité le client est immédiatement mis en communication avec le serveur vocal ou l'opératrice de l'opérateur de télécommunication. Par ailleurs, les fraudeurs n'ont plus la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par l'opérateur de télécommunication et bénéficier de ses services. En effet, les signaux acoustiques d'identification varient à chaque opération. C'est-à-dire chaque fois que la carte est actionnée.

De préférence la dite carte :

- décompte en outre le nombre de fois $C(p,n)$ où elle est actionnée,

30 - émet des signaux acoustiques représentatifs du nombre de fois $C(p,n)$ où elle a été actionnée,

- crypte les signaux acoustiques en fonction du nombre de fois $C(p,n)$ où elle a été actionnée.

De préférence également, les dits moyens informatiques pour traiter et comparer électroniquement les signaux transmis et les données d'identification du client et de la carte détenues par le service informatique de l'opérateur de télécommunication,

- mémorisent le nombre de fois $C(p,m)$ où la carte a été actionnée lors de la dernière opération validée,

- comparent le nombre de fois $C(p,n)$ où la carte a été actionnée, lors de l'opération en cours, avec le nombre de fois mémorisé $N1$,

- rejettent l'opération en cours si $C(p,n)$ est inférieur ou égal à $C(p,m)$ et poursuivent la vérification de l'opération en cours si $C(p,n)$ est supérieur à $C(p,m)$,

- recalculent les signaux électroniques $S'(p,n)$ en fonction des données d'identification et du nombre de fois $C(p,n)$ où la carte a été actionnée, lors de l'opération en cours, puis les comparent aux signaux électroniques $S(p,n)$ transmis. De sorte qu'en cas de coïncidence, l'abonné peut être immédiatement mis en communication avec les services de l'opérateur de télécommunication.

Afin d'augmenter la sécurité, dans une variante de réalisation, le procédé comprend en outre l'étape suivante, l'abonné émet, au moyen d'un clavier associé au combiné téléphonique et/ou à la carte, un code confidentiel. Après transmission au service informatique de l'opérateur de télécommunication, via le réseau de communication, ce code confidentiel est traité et comparé au code confidentiel personnel de l'abonné détenu par le service informatique de l'opérateur de télécommunication.

Ainsi, l'opérateur de télécommunication peut vérifier que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du procédé et d'éviter que le client ne puisse pas contester l'ordre qu'il a passé à l'opérateur de télécommunication, le procédé comprend en outre les étapes suivantes : - les ordres donnés par l'abonné à l'opérateur de télécommunication sont validés par l'abonné en actionnant la carte d'abonné pour qu'elle émette un signal acoustique crypté de validation,

- le dit signal de validation est enregistré par le service informatique de l'opérateur de télécommunication.

Avantageusement, le procédé selon l'invention pourra comporter l'étape complémentaire suivante :

- 5 - un accusé de réception du signal de validation est adressé au client.

Grâce à ce procédé, l'abonné a validé, par une signature électronique, l'ordre qu'il a donné à l'opérateur de télécommunication.

10 L'invention concerne également un système permettant aux abonnés d'un réseau de télécommunication, d'accéder de manière sûre et rapide, aux services que l'opérateur de télécommunication offre à ses clients. Ce système a pour caractéristique de comprendre les moyens de mise en oeuvre du procédé ci-dessus défini et de ses variantes de réalisation.

Plus particulièrement :

- 15 - Le système selon l'invention comprend une carte d'abonné, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte d'abonné et pour chaque abonné, mise à la disposition de ceux-ci par l'opérateur de télécommunication. La dite carte comporte des moyens d'émission de brefs signaux acoustiques d'identification, de type DTMF. Les moyens d'émission sont actionnés par l'abonné au moyen d'un élément accessible de l'extérieur de la carte d'abonné. La carte comporte en outre des moyens de
- 20 cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte est actionnée.

- Le système selon l'invention comprend un combiné téléphonique comprenant un microphone destiné à recevoir et transformer les signaux acoustiques reçus, en des signaux électroniques transmissibles à distance au moyen du réseau de communication.

- 25 - Le système selon l'invention comprend des moyens informatiques, dépendants des services informatiques de l'opérateur de télécommunication, connectés au réseau de télécommunication. Les dits moyens informatiques comprennent :

* une base de données contenant les références des cartes d'abonné et des abonnés et leurs données d'identification,

- 30 * des moyens de traitement et des moyens de comparaison des signaux

électroniques transmis et des données d'identification contenues dans la base de données. Ainsi, grâce à ce système, l'opérateur de télécommunication peut vérifier que l'appelant dispose bien d'une carte authentique et non d'un leurre informatique. Il a pu également identifier le titulaire de la carte comme étant une personne habilitée à utiliser les services qu'il offre. De sorte qu'en cas de conformité le client est immédiatement mis en communication avec le serveur vocal ou l'opératrice de l'opérateur de télécommunication. Par ailleurs, les fraudeurs n'ont plus la possibilité de dérober les données d'identification puisque celles-ci sont transmises automatiquement sous une forme cryptée. En outre, l'enregistrement, sous quelque forme que ce soit, des signaux acoustiques ne sera d'aucune utilité à un fraudeur pour se faire identifier par les services informatiques de l'opérateur de télécommunication. En effet, les signaux acoustiques d'identifications varient à chaque opération. C'est à dire chaque fois que la carte est actionnée.

De préférence la dite carte comporte en outre :

- un compteur incrémental interconnecté aux moyens d'émission et aux moyens de cryptage s'incrémentant d'au moins une unité chaque fois que la carte est actionnée.

De sorte que l'état du compteur incrémental est émis à destination des moyens informatiques et que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental.

De préférence également les dits moyens informatiques comportent en outre :

- des moyens de mémorisation de l'état $C(p,m)$ du compteur incrémental lors de la dernière opération validée.

- des moyens de comparaison de l'état $C(p,n)$ du compteur incrémental émis lors de l'opération en cours avec l'état $C(p,m)$ du compteur incrémental mémorisé.

De sorte que la vérification de l'opération en cours est rejetée si $C(p,n)$ est inférieur ou égal à $C(p,m)$ et est poursuivie si $C(p,n)$ est strictement supérieur à $C(p,m)$.

De préférence également les dits moyens de traitement et les dits moyens de comparaison des signaux électroniques et des données d'identification contenues dans la base de données comportent des moyens permettant de recalculer les signaux électroniques en fonction de l'état $C(p,n)$ du compteur incrémental et des données d'identification puis de les comparer aux signaux électroniques transmis. De sorte qu'en cas de coïncidence,

l'abonné peut être immédiatement mis en communication avec son interlocuteur ou avec les services de l'opérateur de télécommunication.

Afin d'augmenter la sécurité du système, dans une variante de réalisation, le système comprend en outre des seconds moyens de comparaison d'un code confidentiel personnel à l'abonné contenu dans la base de données, à un code confidentiel émis par l'abonné. Ce code est émis au moyen d'un clavier associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques de l'opérateur de télécommunication, par le réseau de communication.

Ainsi, l'opérateur de télécommunication peut vérifier que l'appelant est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le client ne puisse contester l'ordre qu'il a donné à l'opérateur de télécommunication, le système selon l'invention est tel que :

- la dite carte émet, lorsqu'elle est actionnée par l'abonné, un signal acoustique crypté de validation des ordres donnés par l'abonné,
- les dits moyens informatiques comprennent des moyens de détection et d'enregistrement du signal de validation.

Grâce à ce système, le client a validé, par une signature électronique, l'ordre qu'il a donné à l'opérateur de télécommunication.

Avantageusement dans ce cas les moyens informatiques comprennent en outre des moyens d'édition d'un accusé de réception des ordres donnés. Cet accusé de réception est adressé à l'abonné.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variantes de réalisation de l'invention, données à titre d'exemple indicatif et non limitatif, et de :

- la figure 1 présentant une vue schématique en perspective du système et du procédé selon l'invention,
- la figure 2 présentant la carte sous la forme de bloc diagramme,
- la figure 3 présentant l'algorithme de vérification de l'authenticité du signal transmis.

Le système et le procédé selon l'invention permettent au client 11 (autrement désigné sous le nom d'abonné) d'appeler, de manière sûre et rapide, notamment d'une cabine publique 31, au moyen d'un combiné téléphonique 16 comportant un microphone 17, les services 30 que l'opérateur de télécommunication (l'opératrice) 12 met à la disposition de ses clients 11. Le combiné téléphonique 16, situé à distance des services informatiques 18 de l'opérateur de télécommunication, est connecté aux services informatiques 18 via un réseau de communication 15. Le système comprend une carte 10, au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte et pour chaque client 11. Cette carte est mise à la disposition des abonnés de l'opérateur de télécommunication 12.

La carte 10 comporte des moyens d'émission, notamment un haut parleur 13 émettant de brefs signaux acoustiques d'identification 20, de type DTMF. Ces signaux sont émis lorsque les moyens d'émission 13 et les organes qui les contrôlent sont actionnés par le client au moyen d'un bouton 14 accessible de l'extérieur de la carte (non visible sur la figure 1 car situé sur l'autre côté de la carte). Ces moyens d'émission 13 sont excités par un générateur de signaux DTMF 99, contrôlé par un microprocesseur 104 alimenté par une pile 106 et piloté par un résonateur 107. Le microprocesseur 104 contenu dans la carte comporte des moyens de cryptage 103 permettant de crypter, au moins en partie, les signaux acoustiques 20, comportant un algorithme de cryptage 108 et des identifiants 109 spécifiques pour chaque carte 10 et pour chaque client 11, notamment la clé secrète 250 utilisée par algorithme de cryptage 108.

Les signaux acoustiques 20 sont reçus par le microphone 17 du combiné téléphonique, contre lequel le client accole la carte 10. Le système comprend également des moyens de transmission 19 des signaux acoustiques 20, situés dans le combiné téléphonique 16. Ces moyens de transmission 19 transmettent à distance les signaux acoustiques, après traitement et conversion en signaux électroniques, via le réseau de communication 15. Le système comprend également des moyens informatiques 21, dépendants des services informatiques 18 de l'opérateur de télécommunication. Ces moyens informatiques sont connectés au réseau de communication 15 et situés à distance des combinés téléphoniques 16.

Ces moyens informatiques 21 comprennent eux-mêmes :

- une base de données 23 contenant les références des cartes et des clients et leurs données d'identification,

- des moyens de traitement 24 et des moyens de comparaison 25 des signaux électroniques et des données d'identification contenues dans la base de données.

De sorte qu'en cas de conformité, les services 30 de l'opérateur de télécommunication sont immédiatement accessibles au client 11.

De préférence, le microprocesseur 104 et les moyens de cryptage 103 sont conçus de telle sorte que le signal acoustique 20 varie à chaque opération. En effet, crypter un code d'identification c'est le transformer en une suite d'informations, incompréhensibles pour tout un chacun, et que, seul le titulaire de la clef de cryptage, pourra décrypter. Mais cela n'empêche absolument pas la copie du code d'identification crypté, soit au cours de sa transmission acoustique (magnétophone), soit par piratage de la ligne téléphonique. Cette copie utilisée indûment par un fraudeur, sera traitée par le système récepteur comme ayant toutes les caractéristiques de l'original, puis interprétée afin de vérifier les identifiants de la carte.

Le problème posé est donc le suivant : comment rendre impossible toute tentative de reproduction ? Il sera ci-après décrit différentes variantes de réalisation du moyen général qui permet de faire la distinction entre l'original et la copie, lors de l'analyse du signal crypté reçu par les moyens informatiques 21, en insérant un élément distinctif dans le signal 20 du type DTMF émis par la carte 10.

L'une des variantes consiste à utiliser une fonction dite d'horodatage (par exemple, ainsi qu'elle a été décrite dans le brevet US n° 4 998 279). Cette fonction d'horodatage exploite le paramètre "temps" qui évolue en permanence. La "copie" se trouve ainsi en retard, quand elle est émise. Une telle solution nécessite une synchronisation entre les moyens d'émission 13 et les moyens informatiques 21. Pour cela tous les deux doivent disposer d'une "base de temps" et d'un "étalon de fréquence". Ces deux bases de temps ont leur précision propre et leur dérive propre. Il en résulte qu'elles se désynchronisent lentement, mais progressivement. Pour remédier à cette difficulté technique, une certaine dérive est tolérée entre les bases de temps des moyens d'émission 13 et des moyens informatiques

21. Plus cette dérive est importante, plus l'incertitude augmente sur la "validité" de l'information reçue et plus augmente le risque de fraude. Ainsi si une dérive de une minute est tolérée, toute copie illicite de l'émission du signal crypté, et réutilisée frauduleusement dans les 30 secondes qui suivent, sera perçue comme valide par le système d'analyse des moyens informatiques 21.

Une autre variante consiste à utiliser des listes incrémentales (par exemple, ainsi qu'elle a été décrite dans le brevet US n° 4 928 098). Le dispositif d'émission et celui de réception possèdent la liste ordonnée des cryptages successifs du code d'identification ou bien disposent des algorithmes permettant de les établir au fur et à mesure. A un instant donné les moyens informatiques 21 sont en attente du résultat crypté $C(n)$. S'ils reçoivent effectivement le message $C(n)$, il valide l'opération. Mais les moyens informatiques 21 peuvent recevoir un message différent, en effet l'utilisateur de la carte peut avoir actionnée plusieurs fois les moyens d'émission 13 de celle-ci, par jeu, par maladresse, de sorte que la carte est dans la situation d'émettre le résultat crypté $C(n+p)$ lors de sa prochaine utilisation avec les moyens informatiques 21. Si les moyens informatiques 21 reçoivent un message différent, ils cherchent en avant, dans la liste de résultats cryptés successifs, s'il existe un message $C(n+p)$ identique à celui reçu. Pour lever l'ambiguïté "est-ce un message authentique émis par l'émetteur ?" ou "est-ce un message frauduleux ?", la solution consiste à demander ou à attendre l'émission suivante. Si celui-ci est alors identique à $C(n+p+1)$, le système valide alors le message et se place dans l'attente de la prochaine émission, dans l'état $C(n+p+2)$. Si celui-ci est différent, le message n'est pas validé et le système d'analyse reste en attente du message $C(n)$. Une telle variante de réalisation n'est pas très ergonomique puisqu'elle oblige le titulaire de la carte à actionner plusieurs fois celle-ci.

Selon une variante de réalisation préférentielle, pour distinguer le signal original de sa copie, le microprocesseur 104 embarqué dans la carte 10 comporte un compteur incrémental 105. A chaque usage de la carte, le compteur incrémental 105 s'incrémente d'une ou de plusieurs unités. Bien évidemment, telle une roue à cliquet, celui-ci ne peut revenir en arrière, il ne peut qu'avancer à chaque usage.

Dans le cas de cette variante de réalisation, l'état $C(p,n)$ 242 du compteur 105 entre dans

le calcul du message crypté 244 émis par les moyens d'émission 13. La partie codée $S(p,n)$ 241 est calculée par l'algorithme 108 (dont l'équivalent 247 est mémorisé dans les moyens informatiques 21 au moyen de la clé secrète 250 spécifique à chaque carte et de l'état $C(p,n)$ 242 du compteur 105. La carte 10 émet, en plus du numéro d'identification $I(p)$ 240 de la carte et du code d'identification crypté $S(p,n)$ 241, l'état $C(p,n)$ 242 de son compteur incrémental 105 à chaque émission. Les moyens informatiques 21 mémorisent 230, dans la base de données 23, l'état $C(p,n)$ 242 du compteur incrémental 105 lors de la dernière opération validée. Ainsi, à chaque réception de message 244, les moyens de comparaison 25 des moyens informatiques 21 peuvent comparer 245 l'information reçue relative à l'état $C(p,n)$ 242 du compteur 105, à la précédente information reçue $C(p,m)$ 246 et gardée en mémoire 230, 23.

a) - Si l'état $C(p,n)$ 242 du compteur 105 (fig. 2) exprimé dans le message 244 est strictement supérieur ($n > m$) à celui $C(p,m)$ 246 précédemment reçu, alors le message 244 est accepté et l'analyse se poursuit.

b)- Si l'état $C(p,n)$ 242 du compteur 105 exprimé dans le message 244 est inférieur ou égal ($n \leq m$) à celui $C(p,m)$ 246 précédemment reçu, alors le message est refusé. Le message reçu ne peut être qu'une copie antérieurement effectuée ou un leurre informatique.

Si les conditions définies au point a) ci-dessus sont réunies, les moyens informatiques 21 permettent de lire la partie fixe $I(p)$ 240 et de rechercher dans leur propre base de données 23, 230 la clé secrète correspondante de la carte. Les moyens de calcul 239 des moyens de traitement 24 peuvent alors au moyen l'agorithme 247, de l'état du compteur $C(p,n)$ 242 et de la clé secrète $Clé(p)$ 250, procéder au calcul du code crypté attendu par les moyens informatiques 21. Le code crypté $S'(p,n)$ 248 ainsi calculé est comparé 249 à celui effectivement reçu $S(p,n)$ 241, par les moyens de comparaison 25. Ce procédé et ces moyens permettent donc de valider ou d'invalider le message 244, sans qu'il soit nécessaire à l'utilisateur de la carte d'actionner plusieurs fois celle-ci, comme cela est le cas dans la variante de réalisation ci-dessus décrite.

L'existence au sein de la carte 10 d'un compteur incrémental 105 permet, sans coût supplémentaire, de fixer, au moment de la programmation individuelle de la carte, le

nombre maximum de fois où la carte peut être utilisée. Une fois ce maximum atteint, celle-ci n'émet plus de message cohérent et est donc refusée par les moyens informatiques 21.

La trame 244 émise contient, pour une carte donnée (p),

- 5 - une partie fixe I(p) 240 (le numéro d'identification de la carte),
- une partie variable incrémentale C(p,n) 242 (l'état du compteur),
- une partie variable S(p,n) 241 apparemment aléatoire (le résultat d'un algorithme de cryptage 108 sur la clé secrète 250 propre à cette carte (p)).

La trame émise :

- 10 - est toujours différente d'une carte à l'autre,
- est, pour une carte donnée, toujours différente à chaque émission.

Les moyens informatiques 21 permettent, pour une carte donnée (p), de :

- lire la partie fixe I(p) 240 (le numéro d'identification de la carte),
- rechercher dans leur propre base de données 23 la clé secrète 250 de cette carte et le
15 dernier enregistrement reçu de l'état C(p,m) 246 du compteur 105 de cette carte,
- rejeter cette trame 244 si l'état du compteur C(p,n) 242 de l'opération en cours est inférieur ou égal à celui C(p,m) 246 précédemment reçu et de poursuivre la vérification de l'opération en cours si l'état C(p,n) 242 est strictement supérieur à celui C(p,m) 246 précédemment reçu,
- 20 - de "décrypter" le message 244 reçu et d'en valider le contenu, en le recalculant au moyen de l'algorithme de cryptage 247, de la clé spécifique 250 de cette carte et de l'état du compteur C(p,n) 242, puis en comparant le résultat de ce calcul au message reçu.

Ainsi, grâce à cette combinaison de moyens, il est possible d'émettre, au moyen d'une carte ayant le format d'une carte de crédit, des fréquences acoustiques de type DTMF
25 d'identification, recevables par le microphone d'un équipement relié au réseau téléphonique, et d'avoir la certitude de l'authenticité de la carte appelante et d'écarter ainsi tous les fraudeurs utilisant tout enregistrement sonore ou informatique ou tout leurre informatique.

Afin d'augmenter la sécurité du système, dans la variante de réalisation représentée sur la
30 figure 1, les moyens informatiques 21 comprennent en outre des seconds moyens de

comparaison 26. Ces moyens de comparaison permettent de comparer un code confidentiel personnel à l'abonné, contenu dans la base de données, avec le code confidentiel émis par l'utilisateur. Ce code est émis au moyen d'un clavier 27 associé au combiné téléphonique 16 et/ou à la carte 10 et transmis aux moyens informatiques 21 de l'opérateur de télécommunication, par le réseau de communication 15.

Ainsi, l'opérateur de télécommunication a l'assurance que l'appelant 11 est bien la personne habilitée à entrer en relation avec ses services. Une carte volée ne peut pas être utilisée par le voleur faute de connaître le code confidentiel.

Dans une autre variante de réalisation, afin également de renforcer la sécurité du système et d'éviter que le client ne puisse contester l'ordre qu'il a donné à l'opérateur de télécommunication, le système selon l'invention est tel que :

- la carte 10 émet, lorsqu'elle est actionnée 14 par l'abonné, un signal acoustique crypté de validation des ordres donnés par l'abonné 11,
- les dits moyens informatiques 21 comprennent des moyens de détection 21a et d'enregistrement 21b du signal de validation.

Grâce à ce système, le client a validé, par une signature électronique, l'ordre qu'il a donné à l'opérateur de télécommunication.

Avantageusement dans ce cas les moyens informatiques 21 comprennent en outre des moyens d'édition 28 d'un accusé de réception 29 des ordres donnés. Cet accusé de réception est adressé à l'abonné 11.

REVENDICATIONS

1. Procédé permettant à un opérateur (12) de télécommunication d'identifier de manière rapide et de débiter de manière sûre les abonnés d'un réseau téléphonique, le dit procédé comprenant les étapes suivantes :

5 - l'opérateur (12) de télécommunication met à la disposition de chacun des abonnés (11) une carte d'abonné (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque abonné et pour chaque carte d'abonné,

10 - la dite carte (10), au format carte de crédit, émet de brefs signaux acoustiques d'identification, de type DTMF, cryptés au moins en partie, variant à chaque opération, lorsqu'elle est actionnée par l'abonné (11), notamment au moyen d'un bouton (14),

- les signaux acoustiques d'identification sont reçus par le microphone (17) du combiné téléphonique et sont convertis en signaux électriques, avant d'être transmis par le réseau de communication (15) au service informatique de l'opérateur de télécommunication (12),

15 - les signaux transmis et les données de l'abonné et de la carte d'abonné détenues par le service informatique (18) de l'opérateur (12) de télécommunication, sont traités (24) et comparés (25) électroniquement par le service informatique (18) de l'opérateur de télécommunication.

2. Procédé selon la revendication 1

20 - la dite carte (10) :

* décompte (105) en outre le nombre de fois C(p,n) (242) où elle est actionnée (14),

* émet des signaux acoustiques (20) représentatifs du nombre de fois C(p,n) (242) où elle a été actionnée,

25 * crypte (103) les signaux acoustiques en fonction du nombre de fois C(p,n) (242) où elle a été actionnée,

- les dits moyens informatiques (21), pour traiter (24) et comparer (25) électroniquement les signaux transmis et les données d'identification de l'abonné et de la carte détenues (23) par le service informatique (18) de l'opérateur (12) de télécommunication,

30 * mémorisent (230) le nombre de fois C(p,m) (246) où la carte a été actionnée

lors de dernière opération validée,

* comparent (245) le nombre de fois C(p,n) (242) où la carte a été actionnée, lors de l'opération en cours, avec le nombre de fois mémorisé C(p,m) (246)

5 * rejettent l'opération en cours si C(p,n) (242) est inférieur ou égal à C(p,m) (246) et poursuivent la vérification de l'opération en cours si C(p,n) (242) est supérieur à C(p,m) (246),

10 * recalculent (239) les signaux électroniques S'(p,n) (248) en fonction des données d'identification et du nombre de fois C(p,n) (242) où la carte a été actionnée, lors de l'opération en cours, puis les comparent (249) aux signaux électroniques transmis S(p,n) (241),

de sorte qu'en cas de coïncidence, l'abonné peut être immédiatement mis en communication avec les services (30) de l'opérateur (12) de télécommunication.

3. Procédé selon les revendications 1 ou 2, comprenant en outre l'étape suivante :

15 - l'abonné émet, au moyen d'un clavier (27) associé au microphone et/ou à la carte, un code confidentiel ; après transmission au service informatique (18) de l'opérateur de télécommunication, par le réseau de communication (15), ce code confidentiel est traité et comparé (26) au code confidentiel personnel du client détenu par le service informatique de l'opérateur de télécommunication.

20 4. Procédé selon les revendications 1, 2 ou 3, comprenant en outre l'étape suivante :

- les ordres donnés par l'abonné à l'opérateur de télécommunication sont validés par l'abonné en actionnant (14) la carte d'abonné (10) pour qu'elle émette un signal acoustique crypté de validation

25 - le dit signal de validation est enregistré (21b) par le service informatique de l'opérateur de télécommunication.

5. Procédé selon la revendication 4, comprenant en outre l'étape suivante :

- un accusé de réception (29) du signal de validation est adressé au client.

6. Système permettant à un opérateur de télécommunication (12) d'identifier de manière rapide et de débiter de manière sûre les abonnés (11) d'un réseau téléphonique,

30 le dit système comprenant :

- une carte d'abonné (10), au format carte de crédit, personnalisée par des identifiants spécifiques pour chaque carte d'abonné et pour chaque abonné, mise à la disposition de ceux-ci ; la dite carte comportant :

* des moyens (13) d'émission de brefs signaux acoustiques d'identification, de type DTMF, actionnés par l'abonné au moyen d'un élément (14) accessible de l'extérieur de la carte d'abonné,

* des moyens de cryptage permettant de crypter au moins en partie et de varier les signaux acoustiques chaque fois que la carte (10) est actionnée par l'élément (14).

- un combiné téléphonique comprenant un microphone (17) destiné à recevoir et transformer les signaux acoustiques reçus, en des signaux électroniques transmissibles à distance au moyen du réseau de communication (15),

- des moyens informatiques (21), dépendants des services informatiques (18) de l'opérateur de télécommunication (12), connectés au réseau de télécommunication, les dits moyens informatiques (21) comprenant :

* une base de données (23) contenant les références des cartes d'abonnés et des abonnés et leurs données d'identification,

* des moyens de traitement (24) et des moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données, de sorte qu'en cas de coïncidence, l'abonné peut être immédiatement mis en communication avec les services (30) de l'opérateur de télécommunication (12).

7. Système selon la revendication 6,

- la dite carte (10) comportant en outre :

* un compteur incrémental (105) interconnecté aux moyens d'émission (13) et aux moyens de cryptage (103), s'incrémentant d'au moins une unité chaque fois que la carte (10) est actionnée par l'élément (14),

de sorte que l'état du compteur incrémental (105) est émis à destination des moyens informatiques (21) et que les signaux acoustiques sont cryptés en fonction de l'état du compteur incrémental

- les dits moyens informatiques (21) comportant en outre :

* des moyens de mémorisation (23, 230) de l'état C(p,m) (246) du compteur incrémental (105) lors de la dernière opération validée,

* des moyens de comparaison (245) de l'état C(p,n) (242) du compteur incrémental (105) émis lors de l'opération en cours avec l'état C(p,m) (246) du compteur incrémental mémorisé,

de sorte que la vérification de l'opération en cours est rejetée si C(p,n) (242) est inférieur ou égal à C(p,m) (246) et est poursuivie si C(p,n) (242) est strictement supérieur à C(p,m) (246)

- les dits moyens de traitement (24) et les dits moyens de comparaison (25) des signaux électroniques et des données d'identification contenues dans la base de données comportant des moyens permettant de recalculer (239) les signaux électroniques en fonction de l'état C(p,n) (242) du compteur incrémental (105) et des données d'identification puis de les comparer (249) aux signaux électroniques transmis,

8. Système selon les revendications 6 ou 7, les dits moyens informatiques comprenant en outre:

- des seconds moyens de comparaison (26) d'un code confidentiel personnel de l'abonné contenu dans la base de données, à un code confidentiel émis par le client au moyen d'un clavier (27) associé au combiné téléphonique et/ou à la carte et transmis aux moyens informatiques de l'opérateur de télécommunication, par le réseau de communication.

9. Système selon les revendications 6, 7 ou 8, la dite carte émettant en outre, lorsqu'elle est actionnée (14) par l'abonné, un signal acoustique crypté de validation des ordres donnés par l'abonné, les dits moyens informatiques comprenant en outre :

- des moyens de détection (21a) et d'enregistrement (21b) du signal de validation

10. Système selon la revendication 9, les dits moyens informatiques (21) comprenant en outre :

- des moyens d'édition (28) d'un accusé de réception (29) des ordres donnés, destiné à être adressé à l'abonné.

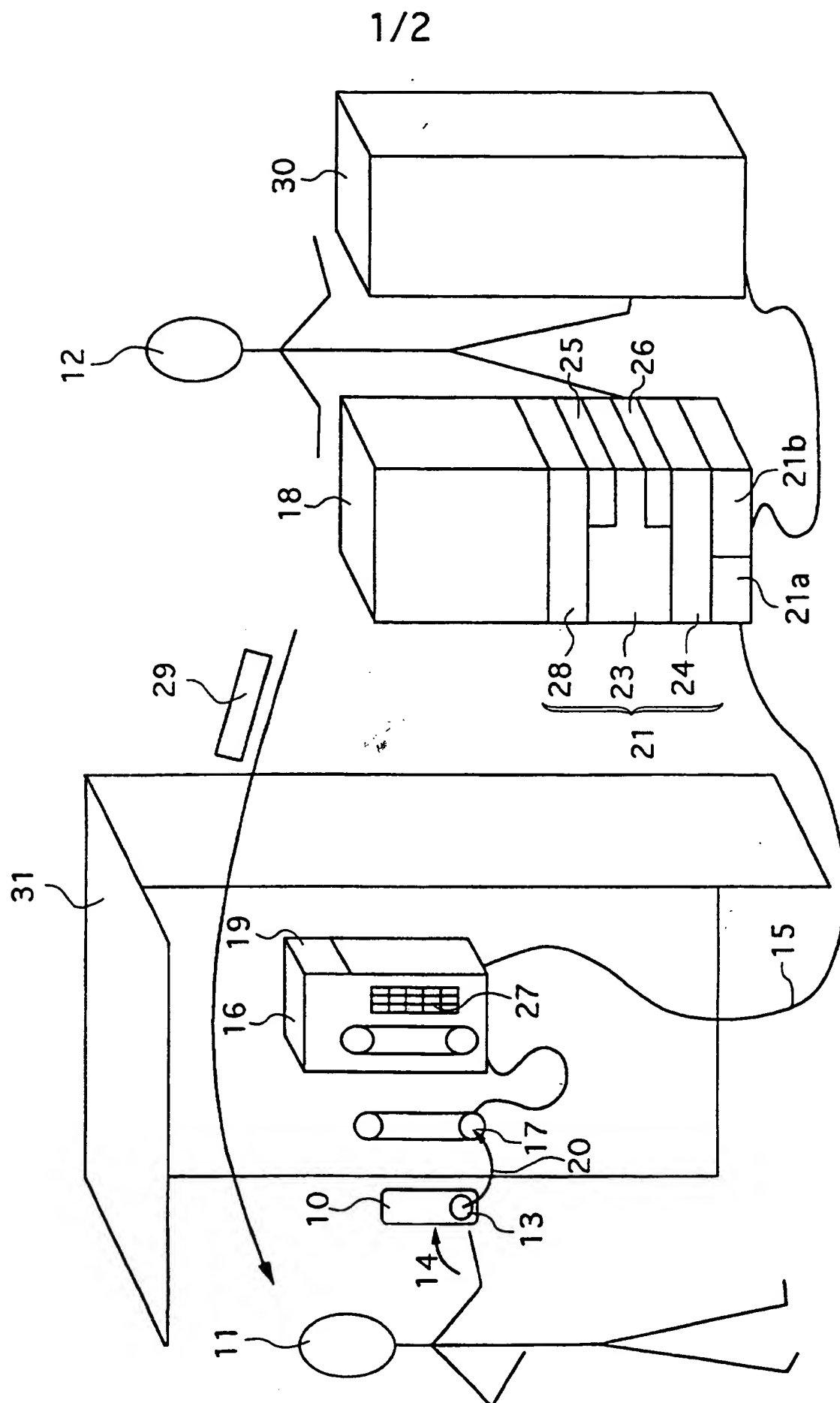


Fig. 1

2/2

